OpsAuditHub opsauditihub.com	DOC ID: **SAF-0155**	REVISION: **Rev 2.4 (2026)**
	STANDARD: **HIPAA Privacy Rule 45 CFR Part 160 and Part 164, Subparts A and E**	AUDIT FREQUENCY: **Quarterly Audit**

Hipaa Privacy Compliance Audit Sop Template

Operational Scope: This Standard Operating Procedure establishes the mandatory protocol for conducting HIPAA privacy compliance audits across all operational healthcare units. The objective is to mitigate protected health information (PHI) exposure risks, enforce administrative and physical safeguards, and ensure total compliance with federal patient privacy mandates.

MANDATORY PPE:	Facility Security Badges, Visitor Identification Lanyards, Confidential Document Shred Bins, Privacy Screen Filters, Asset Tracking Scanners
PREREQUISITES:	Notify clinic practice manager and IT security lead 48 hours prior to audit execution. | Ensure secure access to physical records storage, nursing stations, and electronic health record (EHR) audit logs. | Review previous quarterly audit corrective action logs for open compliance items.

PHYSICAL SECURITY AND WORKSTATION PRIVACY SAFEGUARDS

#	COMPONENT / ITEM	VERIFICATION CRITERIA & ACCEPTANCE STANDARD	SEVERITY	STATUS
1	**Workstation Privacy Filters**	All reception and clinical monitors facing public waiting areas must be equipped with polarized privacy screens preventing unauthorized viewing from side angles.	**Critical (Immediate Out of Service)**	**[ ] PASS [ ] FAIL [ ] N/A**
2	**Unattended Screen Locks**	Active workstations left unattended must engage automatic screen locking mechanisms within a maximum of 3 minutes of inactivity.	**Critical (Immediate Out of Service)**	**[ ] PASS [ ] FAIL [ ] N/A**
3	**Physical Chart and Paper PHI Storage**	Paper charts, intake forms, and printed schedules must not be left exposed on desktop surfaces; storage rooms and file cabinets must remain locked when not actively staffed.	**Warning**	**[ ] PASS [ ] FAIL [ ] N/A**
4	**Visitor Log Controls**	Visitor and vendor logs must be strictly maintained at reception, restricting unescorted access to clinical and administrative back-office zones containing electronic PHI.	**Standard**	**[ ] PASS [ ] FAIL [ ] N/A**

ADMINISTRATIVE SAFEGUARDS AND DOCUMENT DISPOSAL

#	COMPONENT / ITEM	VERIFICATION CRITERIA & ACCEPTANCE STANDARD	SEVERITY	STATUS
5	**Confidential Waste Disposal Receptacles**	Consolidated shredding bins must be securely locked, tamper-evident, and free from overflowing paper waste or visible documents on top.	**Critical (Immediate Out of Service)**	**[ ] PASS [ ] FAIL [ ] N/A**
6	**Notice of Privacy Practices (NPP)**	Current Notice of Privacy Practices must be visibly displayed in the patient reception area and readily available in digital or print formats upon request.	**Warning**	**[ ] PASS [ ] FAIL [ ] N/A**
7	**Role-Based Access Control (RBAC) Review**	Active user accounts in the EHR system must be cross-referenced against current personnel rosters to ensure terminated or transferred staff have had access revoked immediately.	**Critical (Immediate Out of Service)**	**[ ] PASS [ ] FAIL [ ] N/A**
8	**Staff HIPAA Training Compliance Records**	All active clinical, administrative, and volunteer personnel must have documented proof of annual HIPAA privacy and security awareness training on file.	**Warning**	**[ ] PASS [ ] FAIL [ ] N/A**

COMMUNICATIONS AND DISCLOSURE MANAGEMENT

#	COMPONENT / ITEM	VERIFICATION CRITERIA & ACCEPTANCE STANDARD	SEVERITY	STATUS
9	**Verbal Communication and Handoffs**	Staff must utilize lowered voices during patient triage, consultations, and shift handoffs to prevent inadvertent eavesdropping in semi-private or public hallways.	**Warning**	**[ ] PASS [ ] FAIL [ ] N/A**
10	**Patient Authorization and Consent Forms**	Signed disclosures, third-party medical record release requests, and proxy authorizations must be properly filed and verified prior to releasing any PHI.	**Critical (Immediate Out of Service)**	**[ ] PASS [ ] FAIL [ ] N/A**

Certified Compliance Auditor / Privacy Officer Signature: _____	**Date / Time:** _____	**Badge / Cert #:** _____
Clinic Practice Manager / Chief Medical Officer Sign-off: _____	**Review Date:** _____	**Audit Status:** [ ] Approved [ ] Rectify

COMPLIANCE NOTICE: This document must be archived for a minimum of 6 years in accordance with HIPAA administrative simplification recordkeeping guidelines (45 CFR § 164.530).

DIGITAL INSPECTION UPGRADE: Run this audit on mobile/tablet, attach photos & automate compliance records. **Start Free Mobile Audit →**